Приложение № 1

к приказу руководителя Департамента информатизации и связи Забайкальского края от \_\_\_\_\_\_\_\_\_\_\_\_\_\_201\_ г. № \_\_\_\_\_

**Инструкция по организации парольной защиты автоматизированной системы Департамента информатизации и связи Забайкальского края**

*1.Термины и определения*

* 1. **Автоматизированная система (АС) -** система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
  2. **Администратор безопасности информации** - лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.
  3. **Безопасность информации (Информационная безопасность)** - состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.
  4. **Пользователь (потребитель) информации** - субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.
  5. **Первичный пароль** - комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.
  6. **Основной пароль –** комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

1. ***Общие положения***

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах корпоративной сети передачи данных государственных органов Забайкальского края (далее КСПД), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах КСПД контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями в целом возлагается на отдел технической политики и защиты информации Департамента информатизации и связи Забайкальского края (далее ОТПЗИ ДИС ЗК).

В сегментах КСПД исполнительных органов государственной власти Забайкальского края (далее – ИОГВ), а также в информационных системах не имеющих подключения к КСПД и автономных автоматизированных рабочих местах сотрудников за организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей, контроль за действиями исполнителей и обслуживающего персонала возлагается на администратора безопасности информации ИОГВ Забайкальского края.

Администратор безопасности информации обязан регулярно докладывать должностному лицу ИОГВ ответственному за обеспечение безопасности информации о результатах периодической проверки состояния парольной защиты пользователей.

1. *Требования к генерации, использованию, смене и прекращению действия паролей*

**3.1 Установку первичного пароля** производит системный администратор при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе ИОГВ.

Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

При создании первичного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

**3.2 Установку основного пароля** производит **пользователь** при первом входе в систему с новой учетной записью.

Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам отвечающим за информационную безопасность, записывать его в рабочих тетрадях, блокнотах, на элементах оборудования рабочего места, а так же пересылать открытым текстом в электронных сообщениях.

3.3 Личные (основные) пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

Каждый пароль должен выбираться и генерироваться пользователем с учетом следующих требований:

* максимальный срок действия пароля – 6 месяцев (ГОСТ ИСО/МЭК 17799-2005);
* минимальная длина пароля - не менее 8 символов;
* минимальный срок действия пароля – 1 день;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, \*, % и т.п.);
* новый пароль не должен повторять 6 предыдущих значений.

3.4 Пароли к учетным записям, обеспечивающим административный или привилегированный доступ, должны отвечать следующим требованиям:

* максимальный срок действия пароля – 3 месяца (ГОСТ ИСО/МЭК 17799-2005);
* минимальная длина пароля - не менее 12 символов;
* минимальный срок действия пароля – 1 день;
* в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, \*, % и т.п.);
* пароль не должен повторять 8 предыдущих значений.

3.5 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3.6 В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности информации ИОГВ.

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

3.7 Внеплановая смена личного пароля в случае прекращения полномочий работника должна производиться администратором безопасности информации ИОГВ немедленно после окончания последнего сеанса работы данного пользователя с АС.

3.8 Внеплановая смена всех паролей пользователей АС должна проводиться в случае компрометации пароля (потери электронного ключа) администратором безопасности информации ИОГВ.

В случае компрометации личного пароля пользователя АС должны быть немедленно предприняты меры в соответствии положениями настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

3.9 Повседневный контроль за действиями исполнителей и обслуживающего персонала АС при работе с паролями, соблюдением правил их смены, хранения и использования возлагается на администратора безопасности информации ИОГВ. После предоставления текущего значения пароля для проверки на соответствие установленным требованиям контролируемый пользователь обязан сменить свой пароль.

3.10 Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале или конверте (возможно вместе с персональными ключевыми носителями и идентификатором Touch Memory).

3.11 Восстановление забытого основного пароля пользователя (при отсутствии копии на бумажном или другом носителе, п.3.10) осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо зарегистрированной электронной заявки пользователя.

Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

3.12 Для предотвращения угадывания паролей путем подбора системный администратор обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

3.13 Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи *(возможен вариант автоматического разблокирования через продолжительный промежуток времени)*.

3.14 Повседневный контроль за действиями исполнителей и обслуживающего персонала автоматизированной системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в структурных подразделениях ИОГВ (руководителей подразделений), периодический контроль – возлагается на администратора информационной безопасности ИОГВ.

3.15 При наличии (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) технологической необходимости использования имен и паролей некоторых сотрудников в их отсутствие, такие сотрудники обязаны сразу же провести замену личных паролей с заменой их на бумажных и других дублирующих носителях (указанных в п. 3.10).

3.16 Запрещается включение паролей в автоматизированный процесс регистрации, например с использованием хранимых макрокоманд или функциональных клавиш, а также коллективное использование индивидуальных паролей.

1. *Установка пароля на BIOS*
   1. Для исключения угроз безопасности информации, связанной с внедрением вредоносного кода в BIOS, а также перевода BIOS к более ранним версиям, имеющим уязвимости и др. вход в систему BIOS должен быть защищен устойчивым паролем в соответствии с пунктом 3.4 настоящей инструкции.
   2. Пароль на BIOS устанавливается только администратором безопасности информации ИОГВ, значения пароля записываются в специальном журнале, который хранится в опечатанном виде в сейфе (металлическом хранилище) администратора информационной безопасности. Вскрытие журнала производится в присутствии сотрудника, работающего на соответствующем АРМ с записью в журнале, где отражаются дата, время и цель вскрытия.
   3. Замена пароля на BIOS или его сброс производится только с разрешения должностного лица ответственного за информационную безопасность ИОГВ.
2. *Ответственность за нарушение требований настоящей инструкции*

За нарушение требований настоящей инструкции пользователи несут дисциплинарную ответственность в соответствии с действующим законодательством.